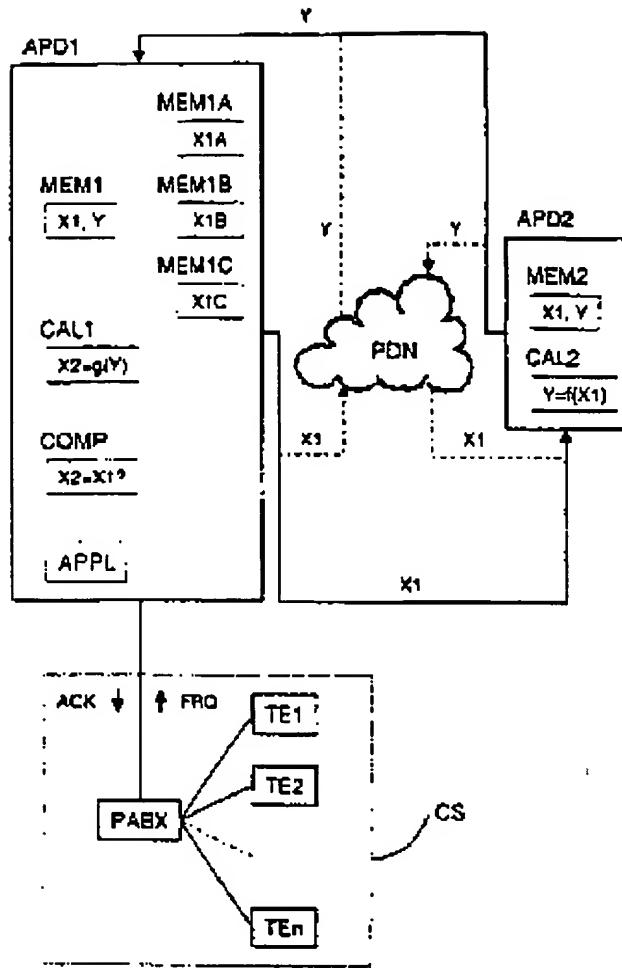


AN: PAT 2002-364408  
TI: Method for transfer of encryption information to register a software application installed on a first computer to a second controlling computer that send back a value that is used to enable authorized application functions  
PN: EP1191419-A2  
PD: 27.03.2002  
AB: NOVELTY - Method for transfer of encryption information to register a software application installed on a first computer (APD1) in which first application data (X1) is transmitted to a second computer (APD2), which sends an application value (Y) back. The first computer uses the application value to calculate second application data (X2). When application execution begins first and second application data are compared and based on the agreement the relevant parts of the application are enabled for use.; USE - Prevention of illegal software copying particularly relevant to software applications distributed via the Internet. ADVANTAGE - Authentication codes are integral with the software and do not have to be entered manually. This speeds up software installation and prevents unauthorized copying. DESCRIPTION OF DRAWING(S) - Figure shows a block diagram of the invention. first and second application program controllers or computers APD1, APD2 first and second application data X1, X2 application value Y application program APPL network PDN communication system. CS  
PA: (SCHU/) SCHULZE K; (SIEI ) SIEMENS AG;  
IN: SCHULZE K;  
FA: EP1191419-A2 27.03.2002; US2003005319-A1 02.01.2003;  
DE10046895-A1 25.04.2002;  
CO: AL; AT; BE; CH; CY; DE; DK; EP; ES; FI; FR; GB; GR; IE; IT;  
LI; LT; LU; LV; MC; MK; NL; PT; RO; SE; SI; TR; US;  
DR: AL; AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;  
LT; LU; LV; MC; MK; NL; PT; RO; SE; SI; TR;  
IC: G06F-001/00; G06F-012/14; H04L-009/28; H04L-009/32;  
H04M-003/42;  
MC: T01-D01; T01-J20B2A; T01-N01D; T01-N02B1B;  
DC: T01;  
FN: 2002364408.gif  
PR: DE1046895 21.09.2000;  
FP: 27.03.2002  
UP: 20.01.2003

BEST AVAILABLE COPY

**THIS PAGE BLANK (USPTO)**



**THIS PAGE BLANK (USPTO)**



(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 191 419 A2

(12)

## EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:  
27.03.2002 Patentblatt 2002/13

(51) Int Cl. 7: G06F 1/00

(21) Anmeldenummer: 01119169.9

(22) Anmeldetag: 08.08.2001

(84) Benannte Vertragsstaaten:  
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
MC NL PT SE TR  
Benannte Erstreckungsstaaten:  
AL LT LV MK RO SI

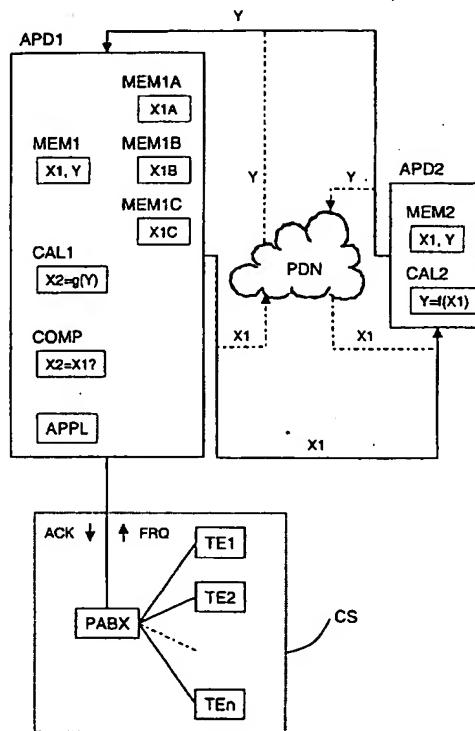
(30) Priorität: 21.09.2000 DE 10046895

(71) Anmelder: SIEMENS AKTIENGESELLSCHAFT  
80333 München (DE)  
(72) Erfinder: Schulze, Karsten  
85390 Hallbergmoos (DE)

(54) Verfahren zur Übermittlung verschlüsselter Informationen zur Registrierung eines Applikationsprogramms

(57) Die Erfindung betrifft ein Verfahren zur Übermittlung verschlüsselter Informationen zur Registrierung eines Applikationsprogramms, das auf einer ersten Programmsteuerungseinrichtung (APD1) installiert ist. Erste Applikationsinformationen (X1) mit zumindest einer gegenüber Benutzerzugriffen gesperrten Teilinformation (X1A) werden an eine zweite Programmsteuerungseinrichtung (APD2) übermittelt. In der zweiten Programmsteuerungseinrichtung (APD2) wird mittels Codierung aus den ersten Applikationsinformationen (X1) ein Applikationswert (Y) berechnet. Der Applikationswert (Y) wird an die erste Programmsteuerungseinrichtung (APD1) übermittelt. In der ersten Programmsteuerungseinrichtung (APD1) werden mittels Decodierung aus dem Applikationswert (Y) zweite Applikationsinformationen (X2) ermittelt. Bei einem Ausführungsbeginn des Applikationsprogramms (APPL) werden die ersten Applikationsinformationen (X1) und die zweiten Applikationsinformationen (X2) auf Übereinstimmung überprüft. In Abhängigkeit der sich bei der Überprüfung ergebenden Abweichungen werden vorgebbare Funktionen des Applikationsprogramms (APPL) freigeschaltet.

Fig.1



## Beschreibung

[0001] Verfahren zur Übermittlung verschlüsselter Informationen zur Registrierung eines Applikationsprogrammes dienen einer Verhinderung von nicht autorisierten Vervielfältigungen des Applikationsprogramms. Derartige Verfahren dienen außerdem als technische Voraussetzung, um Applikationsprogramme als Produkte über E-Commerce zu vertreiben. Bei bisher bekannten Verfahren zur Registrierung von Applikationsprogrammen werden Applikationsprogramme anhand jeweils eines Registrierungsschlüssels freigeschaltet. Für eine Freischaltung eines Applikationsprogramms wird der Registrierungsschlüssel, der einer Applikationsprogrammlizenz fest zugeordnet ist, manuell eingegeben bzw. von einem Datenträger eingespielt. Insbesondere bei einer Vielzahl von auf unterschiedlichem Programmsteuerungseinrichtungen installierten Applikationsprogrammen resultiert hieraus ein hoher Administrationsaufwand, der mit personalintensiven Bedien- und Wartungsarbeiten verbunden ist.

[0002] Der vorliegenden Erfindung liegt die Aufgabe zugrunde, ein Verfahren anzugeben, welches eine automatisierte Registrierung von auf Programmsteuerungseinrichtungen installierten Applikationsprogrammen ermöglicht.

[0003] Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den in Anspruch 1 angegebenen Merkmalen gelöst. Vorteilhafte Weiterbildungen des erfindungsgemäßen Verfahrens sind den abhängigen Ansprüchen zu entnehmen.

[0004] Ein Aspekt des erfindungsgemäßen Verfahrens besteht darin, daß vorgebbare Funktionen eines Applikationsprogramms für eine wählbare Nutzungsdauer durch Modifikation eines Registrierungsschlüsselpaars mit zumindest einer gegenüber Benutzerzugriffen gesperrten Teilinformation freigeschaltet werden können. Die betreffenden Funktionen müssen dabei nicht bereits bei einer Erstinstallation des Applikationsprogramms für eine Freischaltung zur Verfügung gestanden haben. Außerdem ist zur Freischaltung kein Einsatz von Bedien- und Wartungspersonal am Ort der Programmsteuerungseinrichtung erforderlich, auf der das jeweilige Applikationsprogramm installiert ist. Bestandteile des Registrierungsschlüsselpaars sind Applikationsinformationen und ein Applikationswert. Die Applikationsinformationen werden an einer ersten Programmsteuerungseinrichtung eingegeben, auf der das zu registrierende Applikationsprogramm installiert ist, bzw. durch die erste Programmsteuerungseinrichtung generiert. Der Applikationswert wird in einer zweiten Programmsteuerungseinrichtung mittels Codierung aus den Applikationsinformationen berechnet.

[0005] Bei einer Registrierung eines Applikationsprogramms oder einer Änderung der Registrierung werden erste Applikationsinformationen mit zumindest einer gegenüber Benutzerzugriffen gesperrten Teilinformation an die zweite Programmsteuerungseinrichtung übermit-

telt. In der zweiten Programmsteuerungseinrichtung wird aus den ersten Applikationsinformationen ein Applikationswert berechnet, der nachfolgend an die erste Programmsteuerungseinrichtung übermittelt wird. Mit-

5 tels Decodierung werden in der ersten Programmsteuerungseinrichtung aus dem Applikationswert zweite Applikationsinformationen ermittelt. Die ersten und die zweiten Applikationsinformationen werden bei einem Ausführungsbeginn des Applikationsprogramms auf 10 Übereinstimmung überprüft. In Abhängigkeit der sich bei der Überprüfung ergebenden Abweichungen werden vorgebbare Funktionen des Applikationsprogramms freigeschaltet.

[0006] Bei bisher bekannten Verfahren zur Registrierung von Applikationsprogrammen ist eine derartige Vorgehensweise nicht möglich. Anstelle des Registrierungsschlüsselpaars, dessen Bestandteile zwischen der ersten und der zweiten Programmsteuerungseinrichtung ausgetauscht werden, wird dort nämlich lediglich ein Registrierungsschlüssel mit vollständig gegenüber Benutzerzugriffen gesperrten Teilinformationen verwendet.

[0007] Die Erfindung wird nachfolgend an Ausführungsbeispielen anhand der Zeichnung näher erläutert.

25 Es zeigt

Figur 1 eine Anordnung mit einer ersten Programmsteuerungseinrichtung, einer zweiten Programmsteuerungseinrichtung und einem mit der ersten Programmsteuerungseinrichtung verbundenen Kommunikationssystem und

30 35 Figur 2 ein Ablaufdiagramm für ein Verfahren zur Übermittlung verschlüsselter Informationen zur Registrierung eines Applikationsprogramms.

[0008] Die in Figur 1 dargestellte Anordnung weist eine erste Programmsteuerungseinrichtung APD1, eine zweite Programmsteuerungseinrichtung APD2 und ein Kommunikationssystem CS auf. Das Kommunikationssystem CS weist eine Kommunikationsanlage PABX und mehrere an die Kommunikationsanlage PABX angeschlossene Teilnehmergeräte TE1 bis TE<sub>n</sub> auf.

40 45 50 55 Auf der ersten Programmsteuerungseinrichtung APD1 ist ein zunächst noch unregistriertes Applikationsprogramm APPL installiert. Funktionen des Applikationsprogramms APPL sind in diesem Zustand lediglich in eingeschränktem Umfang freigeschaltet. Den Ausgangspunkt für eine Freischaltung weiterer Funktionen des Applikationsprogramms APPL bildet eine benutzer-eingegebene Freischaltungsanforderung. Dabei werden erste Applikationsinformationen X1 durch die erste Programmsteuerungseinrichtung APD1 erfaßt. Dies entspricht Schritt 1 des in Figur 2 dargestellten Ablaufdiagramms.

[0009] Die ersten Applikationsinformationen X1 sind verschlüsselt und verteilt in einer der ersten Programm-

steuerungseinrichtung APD1 zugeordneten Speicher- einrichtung MEM1 abgespeichert. Die Speichereinrich- tung MEM1 weist mehrere MEM1A, MEM1B, MEM1C auf. In den Speicherbereichen MEM1A, MEM1B, MEM1C sind programmsteuerungseinrichtungsbezo- gene Teileinformationen X1A, applikationsprogrammbe- zogene Teileinformationen X1B und benutzerbezogene Teileinformationen X1C der ersten Applikationsinfor- mationen X1 abgespeichert. Die programmsteuerungsein- richtungsbezogenen Teileinformationen X1A sind gegen- über Benutzerzugriffen gesperrt.

[0010] Bei den programmsteuerungseinrichtungsbezo- genen Teileinformationen X1A handelt es sich bei- spielsweise um ein Prozessoridentifikationskennzeichen, ein Netzwerkkartenidentifikationskennzeichen, eine IP-Adresse (Internet Protocol) der ersten Pro- grammsteuerungseinrichtung APD1 oder um sonstige Hardwareidentifikationsmerkmale. Die genannten sind in ihrer Kombination gegenüber Benutzermanipulatio- nen gesichert. Eine Manipulation der genannten Hard- wareidentifikationsmerkmale hat eine erneute Regi- strierung des Applikationsprogramms APPL zur Folge. Eine erneute Registrierung wird nämlich erforderlich, sobald sich ein Identifikationsmerkmal einer Hardware- komponente der Programmsteuerungseinrichtung APD1 ändert.

[0011] Bei den applikationsprogrammbezogenen Teileinformationen X1B handelt es sich beispielsweise um den Hersteller, den Produktnamen, die Produktver- sion oder um freizuschaltende Funktionen des Applika- tionsprogramms APPL. Zu den benutzerbezogenen Teileinformationen X1C zählen beispielsweise der Name, die Adresse oder eine durch den Hersteller des Appli- kationsprogramms APPL vergebene Kundennummer des Benutzers.

[0012] Gemäß Schritt 2 des in Figur 2 dargestellten Ablaufdiagramms werden die ersten Applikationsinfor- mationen X1 an die zweite Programmsteuerungsein- richtung APD2 übermittelt. Dort wird beispielsweise an- hand von Kunden- und Auftragsinformationen über- prüft, ob die Freischaltungsanforderung zulässig ist (Schritt 3). Ist die Freischaltungsanforderung unzulässig, so wird eine Mitteilung über eine Unzulässigkeit der Freischaltungsanforderung an die erste Programm- steuerungseinrichtung APD1 übermittelt (Schritt 10). Außerdem werden die ersten Applikationsinformatio- nen X1 bei einer Unzulässigkeit der Freischaltungsan- forderung in der Programmsteuerungseinrichtung APD1 in ihren Zustand vor der Freischaltungsanforde- rung zurückgesetzt (Schritt 11).

[0013] Ist die Freischaltungsanforderung zulässig, so wird in einer Berechnungseinrichtung CAL2 der zweiten Programmsteuerungseinrichtung APD2 mittels Codie- rung aus den ersten Applikationsinformationen X1 ein Applikationswert Y berechnet (Schritt 4). Zur Berech- nung des Applikationswertes Y aus den ersten Applika- tionsinformationen X1 kann beispielsweise neben dem Blowfish-Algorithmus die Hash-Funktion HAVAL ver-

wendet werden. Zur Protokollierung des Berechnungs- vorganges werden die ersten Applikationsinformatio- nen X1 und der Applikationswert Y in einer Speicherein- richtung MEM2 der zweiten Programmsteuerungsein- richtung APD2 gespeichert. Der berechnete Applikati- onswert Y wird nachfolgend an die erste Programm- steuerungseinrichtung APD1 übermittelt und dort in der Speichereinrichtung MEM1 gespeichert (Schritt 5).

[0014] Die ersten Applikationsinformationen X1 bzw. der Applikationswert Y werden vorzugsweise über ein verbindungslose Dienste bereitstellendes Netz PDN übermittelt. Dies ist in Figur 1 durch die gestrichelten Verbindungen zwischen der ersten Programmsteue- rungseinrichtung APD1, der zweiten Programmsteue- rungseinrichtung APD2 und dem verbindungslose Dien- ste bereitstellenden Netz PDN angedeutet. Die ersten Applikationsinformationen X1 bzw. der Applikationswert Y können damit beispielsweise per E-Mail oder per Pro- grammsteuerungselement (Applet) übermittelt werden.

[0015] In der ersten Programmsteuerungseinrichtung APD1 werden aus dem Applikationswert Y in einer Be- rechnungseinrichtung CAL1 der ersten Programmsteuerungseinrichtung APD1 mittels Decodierung zweite Applikationsinformationen ermittelt (Schritt 6). Nach- folgend wird überwacht, ob ein Ausführungsbeginn des Applikationsprogramms APPL erfolgt (Schritt 7). Bei ei- nem Ausführungsbeginn des Applikationsprogramms APPL werden die ersten Applikationsinformationen X1 und die zweiten Applikationsinformationen X2 in einem Komparator COMP auf Übereinstimmung überprüft (Schritt 8). In Abhängigkeit der sich bei der Überprüfung ergebenden Abweichungen werden vorgebbare Funk- tionen des Applikationsprogramms APPL freigeschaltet (Schritt 9) oder gesperrt (Schritt 12).

[0016] Durch ein Freischalten von Funktionen des Applikationsprogramms APPL werden Leistungsmerk- male im Kommunikationssystem CS aktiviert oder de- aktiviert. Hierzu wird von der Kommunikationsanlage PABX bzw. von einem der Teilnehmerendgeräte TE1 bis TE n eine Leistungsmerkmalanforderung FRQ an die erste Programmsteuerungseinrichtung APD1 übermittelt. Die Leistungsmerkmalanforderung FRQ wird von der ersten Programmsteuerungseinrichtung APD1 als Frei- schaltungsanforderung für ausgewählte Funktionen des Applikationsprogramms APPL behandelt. Bei er- folgter Aktivierung oder Deaktivierung eines Leistungs- merkmals wird eine Quittierungsmeldung ACK an die Kommunikationsanlage PABX übermittelt.

[0017] Die vorliegende Erfindung ist nicht auf die be- schriebenen Ausführungsbeispiele beschränkt.

#### Patentansprüche

1. Verfahren zur Übermittlung verschlüsselter Infor- mationen zur Registrierung eines Applikationspro- gramm, das auf einer ersten Programmsteue- rungseinrichtung (APD1) installiert ist, bei dem

- erste Applikationsinformationen (X1) mit zu mindest einer gegenüber Benutzerzugriffen gesperrten Teilinformation (X1A) an eine zweite Programmsteuerungseinrichtung (APD2) übermittelt werden, 5 **dadurch gekennzeichnet, daß die ersten Applikationsinformationen (X1) programmsteuerungseinrichtungsbezogene Teilinformationen (X1A), applikationsprogrammbezogene Teilinformationen (X1B) und/oder benutzerbezogene Teilinformationen (X1C) aufweisen.**
- in der zweiten Programmsteuerungseinrichtung (APD2) mittels Codierung aus den ersten Applikationsinformationen (X1) ein Applikationswert (Y) berechnet wird, 10
- der Applikationswert (Y) an die erste Programmsteuerungseinrichtung (APD1) übermittelt wird, 15
- in der ersten Programmsteuerungseinrichtung (APD1) mittels Decodierung aus dem Applikationswert (Y) zweite Applikationsinformationen (X2) ermittelt werden, 20
- bei einem Ausführungsbeginn des Applikationsprogramms (APPL) die ersten Applikationsinformationen (X1) und die zweiten Applikationsinformationen (X2) auf Übereinstimmung überprüft werden, 25
- in Abhängigkeit der sich bei der Überprüfung ergebenden Abweichungen vorgebbare Funktionen des Applikationsprogramms (APPL) freigeschaltet werden.

2. Verfahren nach Anspruch 1,  
**dadurch gekennzeichnet, daß die ersten Applikationsinformationen (X1) verschlüsselt und verteilt auf einer der ersten Programmsteuerungseinrichtung (APD1) zugeordneten Speichereinrichtung (MEM1) abgespeichert sind.** 30

3. Verfahren nach einem der Ansprüche 1 oder 2,  
**dadurch gekennzeichnet, daß durch ein Freischalten von Funktionen des Applikationsprogramms (APPL) in einem Kommunikationssystem (CS) verfügbare Leistungsmerkmal aktiviert oder deaktiviert werden.** 35

4. Verfahren nach einem der Ansprüche 1 bis 3,  
**dadurch gekennzeichnet, daß die ersten Applikationsinformationen (X1) und/oder der Applikationswert (Y) über ein verbindungsloses Dienste bereitstellendes Netz (PDN) übermittelt werden.** 40

5. Verfahren nach Anspruch 4,  
**dadurch gekennzeichnet, daß die ersten Applikationsinformationen (X1) und/oder der Applikationswert (Y) per E-Mail übermittelt werden.** 45

6. Verfahren nach einem der Ansprüche 4 oder 5,  
**dadurch gekennzeichnet, daß die ersten Applikationsinformationen (X1) und/oder der Applikationswert (Y) per Programmsteuerungselement (Applet) übermittelt werden.** 50

7. Verfahren nach einem der Ansprüche 1 bis 6,

Fig.1

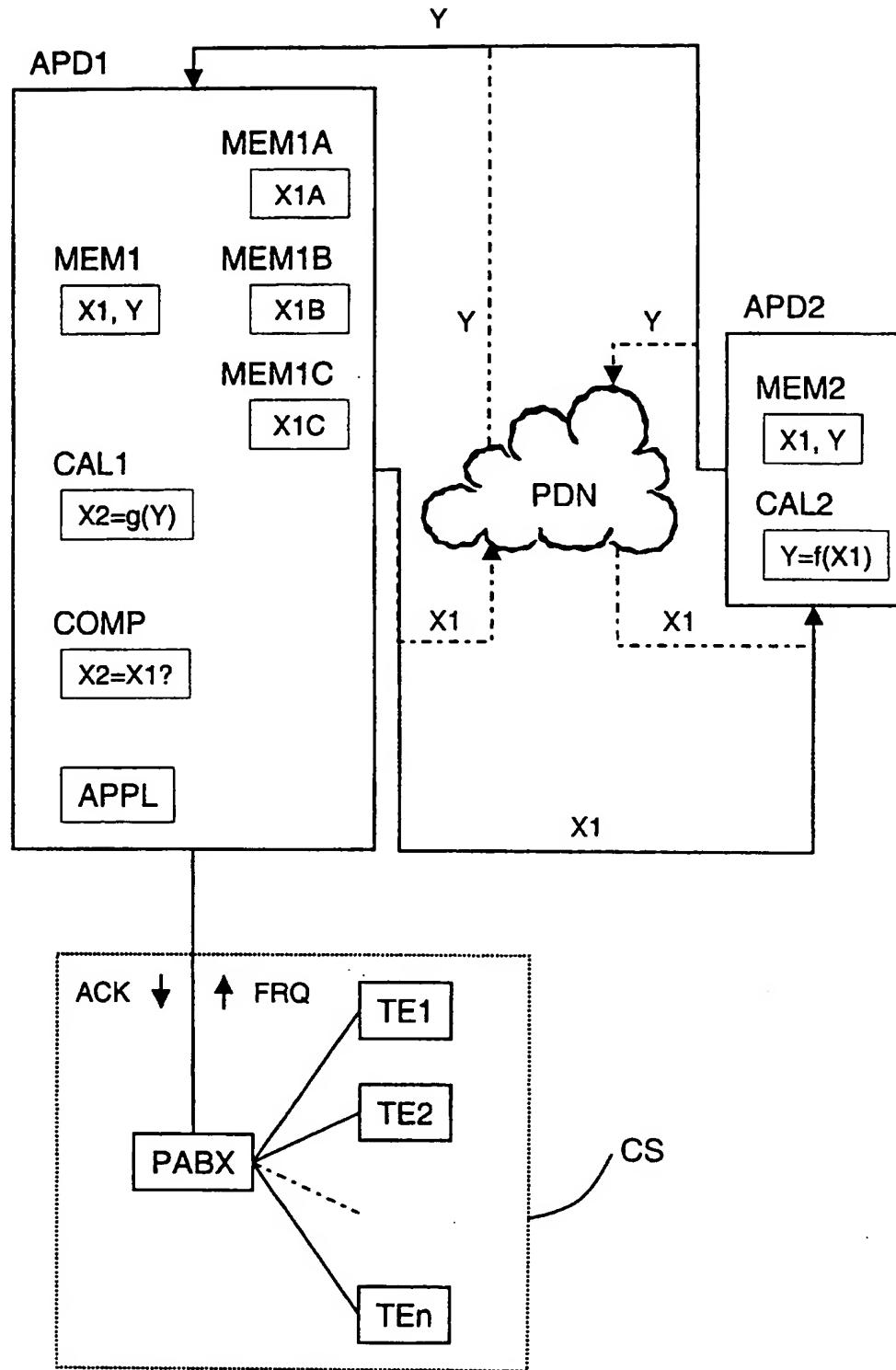
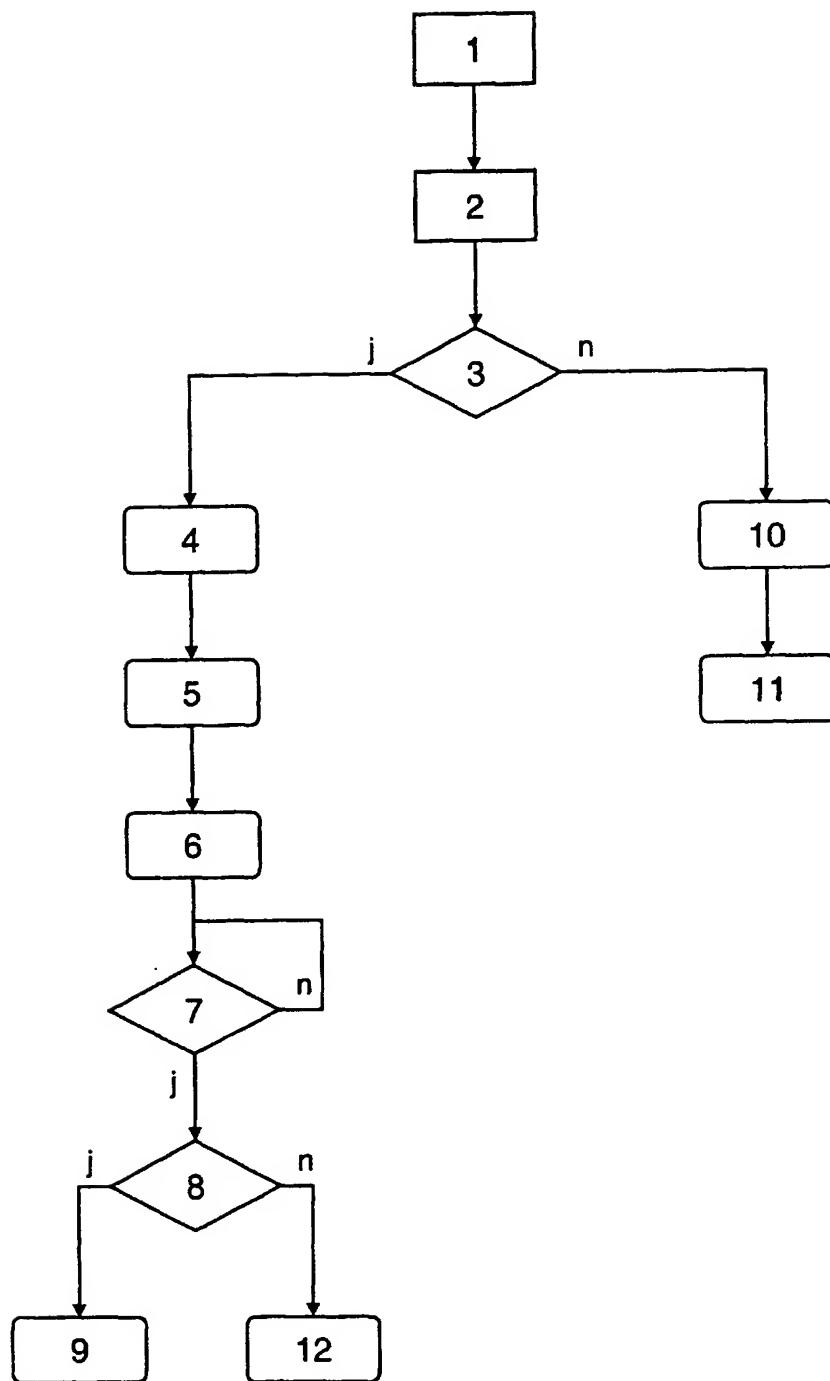
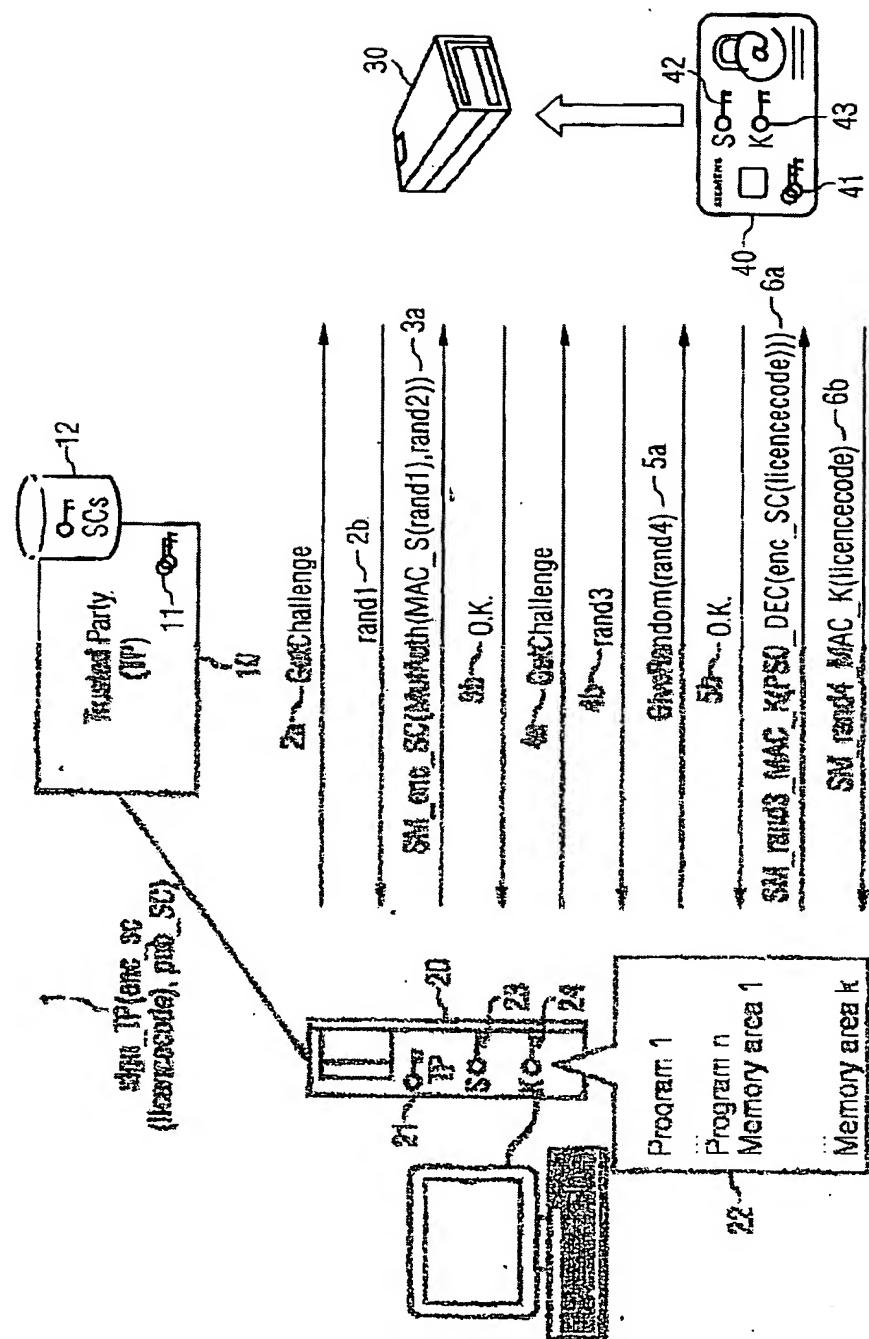


Fig.2



1/1



**THIS PAGE BLANK (USPTO)**

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**